## METHODS FOR PROVIDING INFORMATION ABOUT A PERSON BASED ON FACIAL RECOGNITION

# CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority under 35 U.S.C. § 119(e) to U.S. Provisional Patent Application No. 62/884, 766, filed Aug. 9, 2019. The foregoing application is incorporated by reference herein in its entirety.

### FIELD OF THE INVENTION

[0002] This invention relates to methods and systems for providing information about a person based on facial recognition.

#### BACKGROUND OF THE INVENTION

[0003] In many instances, it may be desirable for an individual to know more about a person that they meet, such as through business, dating, or other relationship. There are many traditional methods to learn about a new person. For example, some of these methods are to ask about the person's background or history, or to receive documentation such as business cards from the person. However, the information provided by the person and this information, either oral or written, could be false. The individual would have little way of determining if the information was accurate or false. Alternatively, one may research the newly met person on a web site or to perform background checks. However, there are many instances when a person can assume a new name or identity to present a false name and history to the individual. As a result, even the best search would not yield accurate results.

[0004] In some situations, the individual needs to know the information about a newly met person right away to determine whether the person is being honest or has the background as asserted. The existing methods are unable to rapidly provide accurate information about the individual. For example, a traditional background check can take from three days to one month. Such delay often renders the obtained information about the person inaccurate and not useful.

[0005] Therefore, a strong need exists for an improved method and system to obtain information about a person and selectively provide the information based on predetermined criteria.

#### SUMMARY OF THE INVENTION

[0006] This disclosure addresses the need mentioned above in a number of aspects. In one aspect, this disclosure presents a method for providing information about a person (e.g., an unknown person, a newly met person, a person with deficient memory). The method includes: (i) receiving facial image data transmitted from a user device. The facial image data comprises at least a captured facial image of the subject; (ii) transforming the facial image data to facial recognition data; (iii) comparing by a server device the facial recognition data to reference facial recognition data associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image; (iv) upon identification of the candidate matching the captured facial image, retrieving from the database personal information (e.g., biography, profile information) associated

with the candidate; and (v) transmitting the personal information to the user device and causing the user device to display the personal information.

[0007] In some embodiments, the method includes preprocessing an image of the subject by the user device. Preprocessing may include detecting a facial image in the image of the subject by the user device. Preprocessing may also include cropping, resizing, gradation conversion, median filtering, histogram equalization, or size normalized image processing. In some embodiments, the facial image is captured by a camera-enabled user device. In some embodiments, the user device is provided in a customized enclosure with an opening for the camera. In some embodiments, the image is captured by a network camera. In some embodiments, the image is imported from a second user device. In some embodiments, the subject is a person. In some embodiments, the subject is a criminal. In some embodiments, the facial image data comprise a three-dimensional facial image of the subject.

[0008] In some embodiments, the method further includes: (i) downloading by a web crawler facial images of individuals and personal information associated therewith; and (2) storing the downloaded facial images and associated personal information in the database. In some embodiments, the reference facial recognition data comprise the facial images downloaded by the web crawler. The reference facial recognition data may include the facial images obtained from the Internet, professional websites, law enforcement websites, or departments of motor vehicles. In some embodiments, the database comprises a plurality of criminal records associated with the facial images stored in the database.

[0009] In some embodiments, the facial recognition data include a vector representation of the captured facial image of the subject. Similarly, the reference facial recognition data may also include a vector representation of the stored facial image in the database. In some embodiments, the vector representation comprises a 512 point vector or a 1024×1024 facial data matrix.

[0010] In some embodiments, the step of comparing further comprises comparing the vector representation of the captured facial image of the subject to a vector representation associated with the stored facial images in the database. Comparing the facial recognition data can be performed by a machine learning module. The machine learning module comprises a deep convolutional neural network (CNN). In some embodiments, identification of the candidate is performed by the k-nearest neighbor algorithm (k-NN).

[0011] In some embodiments, the method may further include detecting a liveness gesture. The liveness gesture is based on at least one of a yaw angle of a second image relative to a first image and a pitch angle of the second image relative to the first image, wherein the yaw angle corresponds to a transition centered around a vertical axis, and wherein the pitch angle corresponds to a transition centered around a horizontal axis.

[0012] In some embodiments, the personal information is retrieved from the database based on a predetermined privacy setting of the identified candidate. In some embodiments, the method further includes displaying one or more facial images of the identified candidate and the personal information associated therewith. In some embodiments, the method may also include transmitting a notification to the user device if the identified candidate poses a high risk to the public or is a criminal. In some embodiments, the personal